Consumer Rights and Protections in the Behavioral Advertising Sector

The collection, use, maintenance, and disclosure of personal and behavioral information for marketing purposes is a threat to consumers' privacy rights. One of the existing structures designed to protect consumers — the self-regulatory Network Advertising Initiative (NAI) — has failed to do so. Marketers and advertising networks may monitor and maintain data on an extensive array of behaviors that a consumer engages in online and in other digital mediums. The expansion of *behavioral tracking* and *targeting* of consumers through the Internet and other networked devices greatly exacerbates the failures of the current inadequate structure for addressing consumer privacy interests.[1] This expansion threatens privacy in new ways that consumers are largely unaware of.

The online *tracking* and *targeting* of consumers — both in its current form and as it may develop in the future — needs to be limited so that consumers can exercise meaningful, granular preferences based on timely and contextual disclosures that are understandable on whichever devices consumers choose to use. Consumers must be free to act in their own self-interest. Companies engaged in monitoring and tracking must respect consumer privacy by implementing Fair Information Practices,[2] and there must be a structure that allows for enforcement of these rights. A right that is selectively enforced, or that is without effective enforcement, is not a meaningful right.

Specifically, we urge the U.S. Federal Trade Commission (FTC) to take proactive steps to adequately protect consumers as online *behavioral tracking* and *targeting* become more ubiquitous.

In particular, the FTC should ensure that the principles of consumer protection the Commission has already begun enforcing on the Internet apply to all areas of online consumer marketing and advertising. These principles include, but are not limited to:

1. **"A consumer's computer belongs to him or her."** "Internet businesses are not free to help themselves to the resources of a consumer's computer."[3]

    - Consumer choice must take precedence. Once a consumer has expressed a choice, an advertiser must not circumvent or

[1] Definitions of *personally identifiable information* (PII), *behavioral tracking*, *behavioral targeting* and other relevant terms are included at the end of this document. Defined terms are italicized throughout the document. For definitions, see p. 6.

[2] Organisation for Economic Co-operation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. September 23, 1980.<http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>.

[3] Remarks of Deborah Platt Majoras, Chairman, Federal Trade Commission, before the Anti-Spyware Coalition, February 9, 2006, p. 5. <http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf>.

override that consumer choice without express notice and meaningful, affirmative consent. For example: A consumer's choice to delete a cookie containing a unique identifier from his or her computer should not be overridden by having the same or a similar identifier reinstated in a new cookie or other *tracking* technology without the consumer's consent.

2. **"Buried disclosures do not work."** "[B]urying critical information in [long disclosure documents] does not satisfy the requirement for clear and conspicuous disclosure."[4]

    - Clear, conspicuous, and highly visible notice must be readily available in context with a behavior being *tracked*. Example: Targeted advertisements could display a link or other mechanism on their face that displays the appropriate notice.

    - Any technologies being used for *behavioral tracking* or *targeting* must be clearly exposed to consumers. Example: The use of secret cookies, tags, and tracking should not be allowed.

    - If an advertiser or another entity offers an opt-out, its implementation by consumers must be persistent, work on all operating systems and platforms in common use, be exercisable using a technology or operation commonly in use, and be generally understood and exercisable by consumers regardless of device type (e.g., personal computer, cell phone, set-top box, etc.). The exercise of an opt-out must be without cost to a consumer.

    - All privacy policies and consumer choices must be robustly, easily, and meaningfully available to all individuals, including those who have visual, hearing, or other disabilities. Standards equal to or greater than the accessibility standards outlined in Sec. 508 of the Rehabilitation Act of 1973 as amended (29 U.S.C. § 794 (d)) should apply.

    - Privacy policies and consumer choices should be easily understandable and accessible to all consumers, including those who are not technical experts.

3. **"If a distributor puts a program on a computer that the consumer does not want, the consumer should be able to uninstall or disable it."**[5]

[4] Majoras, p.7
[5] Majoras, p.8.

- Only the advertiser or entity that stores information in the browser or other network access device should be able to read or modify that information (this is known as the "same-origin principle").[6] This includes cookies and/or any other information an advertiser or entity stores in any part of the consumer's browser, the consumer's computer or device, or network access device.

To help ensure that these principles are followed, the FTC should:

- **Create a national Do Not Track List similar to the national Do Not Call List:**

    - Any advertising entity that sets a persistent identifier on a user device should be required to provide to the FTC the domain names of the servers or other devices used to place the identifier.

    - Companies providing web, video, and other forms of browser applications should provide functionality (i.e., a browser feature, plug-in, or extension) that allows users to import or otherwise use the Do Not Track List of domain names, keep the list up-to-date, and block domains on the list from tracking their Internet activity.

    - Advertisements from servers or other technologies that do not employ persistent identifiers may still be displayed on consumers' computers. Thus, consumers who sign up for the Do Not Track List would still receive advertising.

    - The Do Not Track List should be available on the FTC Web site for download by consumers who wish to use the list to limit tracking.

    - The FTC should engage in public education to disseminate the Do Not Track List information broadly to consumers, along with instructions for its use. The FTC should actively encourage all creators of browsing and other relevant technology to incorporate a facility that will enable consumers to use the list.

- **Ensure that new means of behavioral targeting that defy user expectations receive adequate protections:**

  For example, before allowing or conducting *behavioral tracking*, Internet access providers should provide a consumer with timely, contextual, and robust notice and opportunity to consent before allowing or conducting *behavioral tracking* and sharing the data collected thereby. An Internet access

[6] See Collin Jackson, et.al, "Protecting Browser State from Web Privacy Attacks," WWW 2006, May 23-26, 2006, Edinburgh, Scotland. ACM 1-59593-323-9/06/0005. <http://www2006.org/programme/files/xhtml/3536/index.html>.

provider is any service providing network connectivity and includes but is not limited to an Internet service provider (ISP).

- **Ensure that users are provided with meaningful access to data held about them:**

  Those collecting behavioral data should be required to provide consumers with access to *personally identifiable information* (PII) and other information that is associated with PII retained by the advertiser for *behavioral tracking* and *targeting* uses.

- **Require transparent reporting of industry compliance:**

  Any organization engaged in *behavioral tracking* activities must provide for independent auditing of its compliance with privacy standards. Audit results must be public, except for bona fide trade secrets and *identifiable personal information* about consumers. All audits of a self-regulatory entity or the advertising industry at large should be conducted by a neutral third party, and should be made public in their entirety, not in a condensed form. Consumer complaints to the self-regulatory entity or industry body with company identification should be public, redacted of consumers' *personally identifiable information* (PII). Alternatively, consumer complaints may be added to the FTC Consumer Sentinel database provided that the company information remains subject to public disclosure.

  Advertisers should make full annual compliance reports to the FTC. The FTC should produce an aggregated report (i.e., an Annual Consumer Advertising Protection Report) on the effectiveness of any self-regulatory scheme. The FTC should report annually on the number of companies that are in self-regulatory safe harbors as well as the total number of companies in the industry doing any type of *behavioral tracking* or *targeting*.

- **Urge Congress to establish a national Online Consumer Protection Advisory Committee:**

  Congress should establish a consumer protection advisory committee that would include representatives from state offices of Attorneys General, state and local consumer privacy and consumer protection officials, and consumer and privacy-focused non-profit organizations. The advisory committee would hold regular meetings to evaluate changes in the advertising and consumer marketing sector, including but not limited to new technologies and other changes impacting consumers. The committee would review detailed audit reports from advertisers and industry, and would report problems and suggest solutions to the FTC. The committee would have the ability to hold hearings, and to report its findings to Congress, the FTC, and the public.

- **Promote definitions of important policy terms that can address consumer concerns in online behavioral targeting:**

a. Personally Identifiable Information — Personally identifiable information (PII) consists of any information that can, directly or indirectly:

> (1) identify an individual, including but not limited to name, address, IP address, SSN and/or other assigned identifier, or a combination of unique or non-unique identifying elements associated with a particular individual or that can be reasonably associated with a particular individual, or
>
> (2) permit a set of behaviors or actions to be consistently associated with a particular individual or computer user, even if the individual or computer user is never identified by name or other individual identifier. Any set of actions and behaviors of an individual, if those actions create a uniquely identified being, is considered PII because the associated behavioral record can have tracking and/or targeting consequences.

b. Non-Personally Identifiable Information — Non-Personally Identifiable information (Non-PII) is:

> (1) aggregated data not associated with any individual or any individual identifier, or
>
> (2) any individual level data that is not PII.

c. Behavioral Tracking — The practice of collecting and compiling a record of individual consumers' activities, interests, preferences, and/or communications over time.

d. Behavioral Targeting — Using behavioral tracking to serve advertisements and/or otherwise market to a consumer based on his or her behavioral record.

e. Sensitive Data — Advertisers should not collect, use, disclose, or otherwise process personally identifiable information about health, financial activities, sexual behavior or sexual orientation, social security numbers, insurance numbers, or any government-issued ID numbers for targeting or marketing.

f. Merging of Online and Offline Information – Advertisers should not collect, use, disclose, or otherwise process PII obtained offline with PII obtained online for tracking or targeting purposes unless the consumer has been afforded robust notice and the opportunity to express a preference about such merger before it occurs.

Respectfully submitted to the Federal Trade Commission by:

Ari Schwartz, Deputy Director
Center for Democracy and Technology

Linda Sherry, Director, National Priorities
Consumer Action

Mark Cooper, Director of Research
Consumer Federation of America

Dave Del Torto, Chief Security Officer
The CryptoRights Foundation

Lee Tien, Senior Staff Attorney
Electronic Frontier Foundation

Deborah Pierce, Executive Director
Privacy Activism

Daniel Brandt, President
Public Information Research

Robert Ellis Smith, Publisher
Privacy Journal

Beth Givens, Director
Privacy Rights Clearinghouse

Pam Dixon, Executive Director
World Privacy Forum